WHAT IS CLAIMED IS:

1. In an environment that includes a plurality of users , wherein each user possesses secrets that are shared by respective sets of said plurality of users, a secret updating method, comprising:

(a) updating at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user.

2. The method of claim 1, wherein said updating comprises updating a plurality of compromised secrets.

3. The method of claim 1, wherein said updating comprises updating all compromised secrets.

4. The method of claim 1, wherein said updating comprises updating at least one compromised secret known by one evicted user.

5. The method of claim 4, wherein said updating occurs upon an eviction event.

6. The method of claim 1, wherein said updating comprises updating at least one compromised secret known by a plurality of evicted users.

7. The method of claim 6, wherein said updating occurs on a periodic basis.

8. The method of claim 1, wherein said updating comprises updating a compromised secret using one non-compromised secret.

9. The method of claim 1, wherein said updating comprises updating a compromised secret known by a set of users using a non-compromised secret of a subgroup of said set of users.

10. The method of claim 1, wherein said updating does not use new secret information.

11. The method of claim 1, wherein said compromised secret is shared by said plurality of users.

12. The method of claim 1, wherein said secrets enables secure communication.

13. In an environment that includes a plurality of users , wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of users, said set of users including at least said first user and a second user, a keying method, comprising:

(a) upon eviction of at least said second user, determining an updated first key using information that includes said first key and a second key, wherein said second key enables secure communication among a subgroup of said set of users, wherein said subgroup does not include users subject to said eviction.

14. The method of claim 13, wherein only said second user is evicted.

15. The method of claim 13, wherein said second user and one or more other users in said set of users are evicted.

16. The method of claim 13, wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key.

17. The method of claim 16, wherein said determining uses a one-way function.

18. The method of claim 17, wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function.

19. The method of claim 13, wherein said determining uses only said first key and said second key.

20. The method of claim 13, wherein said subgroup includes only said first user.

21. The method of claim 13, wherein said subgroup includes a plurality of users.

22. A keying method, comprising:

(a) distributing information that enables each of a plurality of users to determine an individual set of keys, wherein each individual set of keys enables a respective user to securely communicate with a plurality of sets of said users; and

(b) upon eviction of at least one user, sending a message to each user that has a set of keys that includes one or more compromised keys known by said at least one evicted user, said message identifying users subject to said eviction and initiating a rekeying process by non-evicted users to modify compromised keys using non-compromised keys that are not known by said at least one evicted user.

23. The method of claim 22, wherein said distributed information includes said individual set of keys.

24. The method of claim 22, wherein said distributed information enables users to generate individual sets of keys.

25. The method of claim 22, wherein only one user is evicted.

26. The method of claim 22, wherein a plurality of users is evicted.

27. The method of claim 22, wherein said plurality of sets of users includes a set of all users.

28. A keying method in an environment having a plurality of users , each user being capable of storing a set of keys that enable secure communication among sets of said plurality of users, comprising:

(a) distributing first information that enables users to update, after eviction of one or more users, a set of compromised keys that are known to said one or more users without receiving new key information.

29. The method of claim 28, wherein said first information includes information that enables identification of a one-way function.

30. The method of claim 28, wherein said first information includes information that enables identification of said evicted one or more users.

31. A keying method in an environment having a plurality of users, comprising:

(a) distributing first information to a user, said first information enabling said user to store a plurality of pieces of information, each of said plurality of pieces of information being associated with a respective set of said plurality of users; and

(b) distributing second information to said user, said second information enabling said user to identify one or more users in a first set of users that have been evicted, wherein said user uses a piece of information that is associated with a subgroup of said first set of users that does not include said evicted members to generate a new key for said first set of users.

32. The method of claim 31, wherein said first information is information that enables said user to derive a plurality of keys.

33. The method of claim 31, wherein said first information is a plurality of keys.

34. The method of claim 31, wherein said plurality of pieces of information is key information.

35. The method of claim 31, wherein said second information identifies one evicted user.

36. The method of claim 31, wherein said second information identifies a plurality of evicted users.

37. The method of claim 31, wherein one of said plurality of pieces of information is associated with a set that includes said plurality of users.

38. A secret sharing system, comprising:

a key server that distributes secret information to a plurality of users, wherein each user is sent secrets that are shared by respective sets of said plurality of users, said key server being operative to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user.

39. A computer program product, comprising:

computer-readable program code for causing a computer, in an environment that includes a plurality of users, wherein each user possesses secrets that are shared by respective sets of said plurality of users, to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user; and

a computer-usable medium configured to store the computer-readable program codes.